ISSN: 2661-3719(Print); 2661-3727(Online)

计算机网络病毒与计算机网络防范安全

刘相汝　朱秋霖
辽宁科技大学　辽宁　114051

摘　要：近些年来，在科学技术快速发展的推动下，计算机网络技术也得到了快速的发展，同时计算机网络技术在各个行业的发展中都得到了大规模的推广使用，同时也产生了非常好的应用效果。但是，随着对计算机网络技术应用和研究的不断加深，网络时代中存在的问题也逐渐暴露出来，其中网络型病毒就是现阶段一个必要重要的问题。计算机网络病毒的存在，不仅会对个人信息造成威胁，严重的话还会带来巨大的经济损失，因此我们必须也要给予计算机网络安全防范工作足够的重视，要能够针对现阶段存在的网络安全问题，采取积极有效的控制措施，使计算机网络病毒得到有效控制的同时，能够给计算机网络运行创造一个良好的环境。

关键词：计算机；网络病毒；安全防范

1　引言

计算机网络的出现，使得电脑得到了大范围的推广与使用。对于电脑来说，由于其有着较强的逻辑性、运算能力以及精准性，并且还有着非常强大的数据存储能力，因此成为了现阶段各个行业发展中都不可或缺的重要设备。但是，需要注意的是，虽然计算机技术和相关的设备能够给我们的生产生活带来巨大的便利，但是也会带来不利的影响。对于计算机网络技术来说，其本身也存在着一定的安全漏洞。在计算机技术快速发展的过程中，病毒的种类也发生了巨大的变化，直至今天计算机病毒不管是在传染性还是危害性上，都有着巨大的提升。

2　计算机网络病毒概述

当前阶段的计算机网络病毒，大多数都是以web服务器、邮件、文件共享为渠道来实现大范围传播的，随着计算机网络病毒的不断发展和更新，当前阶段的新病毒，不仅传播途径广其传播速度和危害性都得到了大幅的提升，并且在传播的过程中也是难以被发现的。计算机网络病毒所具有的特性有以下几点：（1）有着较强的传染性。现代化的计算机网络病毒有着难以想象的繁殖能力，在互联网技术的推动下，虽然可以实现网络用户之间的数据共享，但是共享行为和平台的存在，也给病毒的传播和蔓延提供了良好的机会；（2）有着较强的破坏性。现阶段计算机病毒的种类是比较多的，因此病毒之间的传染能力和破坏能力都有着较大的差异[1]，其中有一小部分的病毒仅仅是对系统的正常运行带来一定的影响，而不会对软件造成不必要的破坏，但是也有一部分的计算机病毒会对软件运行过程中的部分程序和数据信息造成破坏，并且会导致其无法正常还原。另外也有一部分危害程度较大的计算机软件，会直接摧毁整个运行系统，带来无法挽回的损失与影响[1]；（3）有着较强的潜伏性。对于大多数的计算机病毒来说，都能够长期潜伏在计算机程序或者相应的文件中，当病毒处于潜伏期时，并不会对系统的稳定运行带来不利影响，在潜伏期间，病毒的繁殖都是悄无声息的进行，很难被察觉，一旦达到某个触发条件后，病毒就会大规模的爆发，其破坏力是显而易见的。

3　网络病毒的传播方式及影响网络安全的因素

对于大多数的计算机网络病毒来说，可以进行直接的解释和执行操作，也正是因为这种特性的存在，使得计算机网络型病毒有着极其简单的感染方式。现阶段，一些常见病毒的传播途径主要有三种，其一是可以在文件的传输与接受的过程中进行传输；其二在电子邮件传输和发送的过程中进行传播；其三可以在浏览网站的过程中实现传播。其中邮件传播和网站传播最为常见，但是仍以邮件传播的方式为主。对于邮件传播途径来说，大多数的计算机病毒都是通过隐藏在邮件附件中，一旦用户发出附件的执行命令，就会导致病毒发作，甚至有部分的病毒会直接隐匿在邮件中，一旦用户下载并浏览邮件，就会导致中病毒问题的出现。对于网络系统的安全来说，指的就是整个网络硬件、软件运行过程中的安全，同时软硬件中的数据安全也能够得到可靠的保障，能够使整个系统都处于正常、稳定的运行状态中。对于计算机网络运行过程可能存在的病毒威胁来说，主要内容如下：（1）指令上的错误、删除修改数据的过程存在错误、系统配置过程缺乏合理性等人为操作失误；（2）自然灾害的影响；（3）计算机病毒；（4）人为影响因素下的主动入侵和攻击；（5）计算机操作系统、应用软件以及各种通讯协议上存在相应的安全漏洞[2]。

对于这些影响计算机网络运行安全的因素来说，主要就是通过信息安全和系统安全两个方面来呈现的。因此，在针对现阶段存在的网络安全问题时，我们要能够把安全防护重点放在针对病毒和漏洞的防治上，要能够通过科学有效的措施，来使计算机网络能够处于一个相对安全的运行环境中，从而能够发挥其最大的应用价值。

4 计算机网络安全防范措施

4.1 相关技术的充分应用

针对现有的计算机网络安全问题，我们必须要针对相关的问题和漏洞，采取相应的控制措施。为了给计算机的运行创造一个良好的网络环境，并且使其能够处于最佳的运行状态中，我们要能够加强对相关安全防范技术的研究力度，要能够在现有技术体系的基础上，进行更加深入的优化与创新。首先就是要能够加强对防火墙技术的研究和应用，对于防火墙技术来说，由于其本身有着较强的综合性，因此能够通过对网络出入权限的有效把控，来实现对全部网络链接的全面检查，进而能够使外界因素对网络带来的破坏和干扰程度降至最低，另外防火墙技术作为一种比较特殊的隔离控制技术，通过对该技术的灵活使用，能够在不安全网络和机构网络之间形成一道屏障，在屏障的阻隔之下，能够实现对那些非法访问组织的控制，从而能够达到防止网络重要数据非法输出的目的。对于多数的企业来说，只要企业网和互联网之间存在相应的防火墙软件，就能够使内部信息系统的安全性得到可靠的保障；除了防火墙技术以外，入侵检测技术也是非常重要的一种计算机网络安全防范技术手段[3]。对于入侵检测技术来说，其又被称为网络实时监控技术，该技术是通过对计算机网络系统中多个关键点信息的收集与分析，来对网络中存在的入侵现象进行寻找的。因此，从技术应用的整体性上来看，入侵检测技术不仅具备安全监控、审计以及攻击识别等多种功能，在实现安全防护的基础上，还能够使整个计算机系统的网络安全管理能力得到巨大的提升。另外，在入侵检测系统的应用下，还能够对本身的网络系统以及用户的活动等内容进行更加全面、有效的监控与研究，同时还能够通过对系统和关键数据文件完整情况的分析与判断，来发现计算机网络中存在的违反网络安全管理规定的行为。

4.2 注重计算机网络管理

在采取措施加强对计算机网络的管理时，要能够针对计算机网络的每一个具体的环节，采取相应的管控措施，同时还要能够制定科学、完善、有效的管理制度，用制定限制的方式来提高计算机网络管理的质量。另外，为了使系统运行的安全性和稳定性得到可靠的保障，还要能够安排专业的工作人员来对计算机网络进行实时的监控，一旦发现病毒就能够及时采取措施进行防控。

4.3 身份认证与访问控制

对于处于网络环境中的每一台计算机设备来说，都要能够通过相应的身份认证措施来实现对相关信息的识别，对于部分访问情况来说，则要能够站在身份辨认的角度上来对其进行确认。因此对于计算机网络安全管理人员的管理工作，就提出了较高的要求。首先要能够设置相应的口令，通过对口令的认证来实现对整个访问系统的控制。另外，还要能够结合实际情况，针对不同的用户，采取分层管理措施，从权限管理的角度来实现对网络资源的充分利用。对于口令认证来说，则可以通过对字符数的管控，利用字符之间的组合关系设定相关的口令。当前阶段的网络认证环境相对来说是比较复杂的，因此口令认证也存在着一定的安全风险。对于网络身份认证工作来说，整个认证环节是极其复杂的，在主机平台上对双方的身份进行认证处理时，则需要通过网络平台来开展相应的操作，此时的网络系统就会给黑客的入侵提供便利。在面对此类计算机网络安全问题时，可以通过采取秘钥加密的方式来进行处理。

4.4 反病毒软件

不管采用的是密钥认证技术、数据加密技术还是病毒防火墙技术，由于其技术的实现都需要依赖计算机网络环境，因此给病毒和黑客的入侵提供了便利。同时，随着互联网技术的不断发展，网络病毒的变异速度也在不断加快，这也在一定程度上使得病毒感染的概率大幅提升。因此，除了可以采用一些常用的技术手段来加强把控以外，还可以利用一些反病毒软件来实现对病毒的有效控制。对于反病毒软件来说，在通过对网络病毒科学分析检测的基础上，能够使一些恶意的程序行为得到预防与控制，因此能够使整个网络安全和管理工作的质量得到大幅的提升。例如，我们可以通过在NT服务器上安装杀毒软件，来实现对本局域网的全部设施进行安全配置，同时还能够在操作系统间相关安全处理措施的应用下，建立一套更加全面、完善的网络病毒防御系统。另外，还可以结合反病毒软件的一些基本特点，来开展目标特性的设计，这样在发现病毒时，就能在最短的时间内启动病毒隔离系统，此时如果个别终端系统或者是软件存在病毒感染问题的话，那么安装了反病毒软件的服务器就能够对病毒起到一个隔断的作用。

5 结束语

总而言之，在科学技术快速发展的推动下，计算机技术也得到了进一步的优化与创新，但是在此过程中网络安全问题的漏洞也越来越多，因此我们要能够给予网络安全防范足够的重视，要能够针对现有的病毒问题和病毒传播途径，采取科学有效的措施，在解决病毒传播及系统漏洞问题的基础上，还能够为计算机的运行创造一个安全的网络环境。

参考文献：

[1]储佳.探究计算机网络病毒与计算机网络防范安全[J].军民两用技术与产品，2017（4）：2.

[2]刘建辉.计算机网络安全与计算机病毒防范措施浅析[J].网络安全技术与应用，2017（1）：2.

[3]刘昱红.计算机网络安全与计算机病毒防范措施研究[J].中国新通信，2020.